el/2005R00946

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	: Hon.
	:
v.	: Criminal No. 09- 103 (SDW)
	:
EDWIN ANDRES PENA a/k/a "Javier Alejandro Sanchez Rinco," a/k/a "David Hauster," a/k/a "Renato Moreno"	: 18 U.S.C. §§ 371, 1030, 1343 and 2

INDICTMENT

The Grand Jury in and for the District of New Jersey, sitting at Newark, charges:

COUNT ONE
CONSPIRACY
(18 U.S.C. § 371)

BACKGROUND

1. At various times relevant to this Indictment:

a. Edwin Andres Pena ("defendant PENA"), was a citizen of Venezuela and resided in Miami, Florida. Defendant PENA held himself out publically as a telecommunications security expert, capable of identifying and addressing security vulnerabilities of computer networks of telecommunications businesses. Defendant PENA also controlled and operated two telecommunications companies known as Fortes Telecom, Inc. ("Fortes Telecom") and Miami Tech & Consulting, Inc. ("Miami Tech") out of two residences located in Miami. When transacting business on behalf

of Fortes Telecom and Miami Tech, defendant PENA communicated via e-mail, using the address "e_andres55@hotmail.com" ("defendant PENA's E-Mail Address").

b. Fortes Telecom, incorporated in the State of Florida on or about September 14, 2004, purported to be a legitimate wholesale provider of Voice Over Internet Protocol ("VoIP") telephone call service. Through Fortes Telecom, defendant PENA offered and sold millions of minutes of VoIP telephone call service to various telecommunications companies with whom he contracted at steeply discounted below market rates.

c. Miami Tech, incorporated in the State of Florida on or about September 27, 2005, purported to be in the business of providing VoIP auditing and security consulting. According to its web-site, http://www.miamitac.com, Miami Tech provided "VoIP Security Auditing." Defendant PENA used Miami Tech to contract with various telecommunications companies for the sale of millions of minutes of VoIP telephone call service at steeply discounted, below-market rates.

d. Robert Moore ("Moore"), a coconspirator not named as a defendant herein, resided in Spokane, Washington. Moore held himself out publically to be a computer programmer and professional computer hacker. Moore produced software applications capable of gaining unauthorized access to computer

networks and hardware devices and advertised such software on his website, http://www.moorer-software.com.

e. The company identified herein as "O.H." was an investment services company with offices located in or around Ryebrook, New York and had a network router that was connected to the internet and served the function of directing incoming and outgoing internet data and communications.

f. The companies identified herein as "L.N.," "N.T," "R.S.," "N.C.," "G.T.," "G.T.T.," "V.E.," and "N.P." (the "VoIP Telecom Providers") were VoIP telephone service providers that provided telephone services utilizing the internet for transmissions of its communications. N.P. corporate offices were located in or around Newark, New Jersey. The VoIP Telecom Providers accepted VoIP telephone calls from other telecommunications businesses and transmitted those calls to the intended recipients' local telephone carriers via the internet.

2. VoIP services permitted telephone calls to be converted to digital signals and then transmitted through broadband internet connections rather than telephone wires. The digital signals were then converted back to a voice signal at the destination. VoIP signals did not typically travel directly from sender to recipient, but rather were routed through intermediate VOIP carriers who charged different rates for transmitting the signals. To take advantage of the lowest rates, the

telecommunications industry used "least-cost-routing." Utilizing least-cost routing, a VoIP telephone call would be routed through a number of different VoIP carriers before reaching the final destination, with each carrier offering the least expensive rate for carrying the call forward. Each telecommunications company was billed by a subsequent telecommunications company which transmitted the VoIP call forward to its destination.

THE CONSPIRACY

3. From in or about November 2004 through in or about May 2006, in Essex County, in the District of New Jersey and elsewhere, defendant

EDWIN ANDRES PENA
a/k/a "Javier Alejandro Sanchez Rinco,"
a/k/a "David Hauster,"
a/k/a "Renato Moreno"

did knowingly and intentionally conspire and agree with Robert Moore and others to commit an offense against the United States, that is:

(1) to devise a scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and to transmit and cause the transmission by means of wire communications writings, signs, signals, and sounds in interstate and foreign commerce, in furtherance of such scheme and artifice, contrary to Title 18, United States Code, Section 1343; and

(2) to access a protected computer, without authorization, and exceed authorized access, and by means of such conduct to further the intended fraud and obtain things of value, contrary to Title 18, United States Code, Section 1030(a)(4).

OBJECT OF THE CONSPIRACY

4. It was the object of the conspiracy to sell VOIP telephone service to telecommunications companies (the "Telecom Customers") and then route the corresponding telephone calls from the Telecom Customers over hacked computer networks of telecommunications companies without paying those companies for the service they provided.

MANNER AND MEANS OF THE CONSPIRACY

5. It was part of the conspiracy that, from as early as in or about November 2004 to in or about May 2006, unbeknownst to the Telecom Customers, rather than legitimately purchasing VoIP telephone routes for resale, defendant PENA, Moore, and others would create what amounted to "free" telecommunications routes by surreptitiously hacking into the computer networks of the unwitting VoIP Telecom Providers and routing the Telecom Customers' calls, constituting interstate wires, through the VoIP Telecom Providers' networks in such a way so as to avoid detection.

Avoiding Detection: Hacking Computers of Intermediaries, Establishing Decoy Servers, and Using IP Eliminator

6. It was further part of the conspiracy that, in order to avoid detection when establishing the "free" calling routes, defendant PENA would recruit others, including Moore, to perform scans of computer networks of unsuspecting companies and other entities in the United States and worldwide, searching for vulnerable ports where computer networks could be hacked (the "Unsuspecting Intermediaries").

7. It was further part of the conspiracy that after the coconspirators identified vulnerable computer networks of Unsuspecting Intermediaries, Moore would deliver to defendant PENA's E-Mail Address information that he obtained through hacking, including the types of routers used, usernames, and passwords, all of which were necessary to infiltrate their networks.

8. It was further part of the conspiracy that after receiving the information from Moore, defendant PENA would reprogram the Unsuspecting Intermediaries' computer networks to accept VoIP telephone call traffic. Defendant PENA would then route the VoIP calls of his Telecom Customers through the Unsuspecting Intermediaries' networks. In this manner, defendant PENA would make it appear to the VoIP Telecom Providers that the calls were coming from the Unsuspecting Intermediaries' networks and avoid being billed for those calls.

9. It was further part of the conspiracy that Moore and defendant PENA would use various methods to avoid detection. For example, defendant PENA and Moore would arrange to use computer servers hosted at FDCServers, Netsonic and other internet service providers using false names, including "David Haust," "Jake Hamilton" and "Renato Moreno" (the "Decoy Servers"). Defendant PENA would then route VoIP calling traffic of the Telecom Customers through the Decoy Servers, thereby further misleading the VoIP Telecom Providers concerning the origin of the calls. In an effort to avoid creating a traceable paper trail, the coconspirators paid for the Decoy Servers with money orders rather than by check or credit card.

10. It was further part of the conspiracy that defendant PENA would attempt to avoid detection by subscribing to a service known as IP Eliminator which concealed the identity of the computer used to connect to the internet. In this way, the coconspirators were able to conceal the location of the computers that they used to hack into the networks of the Unsuspecting Intermediaries and VoIP Telecom Providers.

Sending the Calls:
Hacking into VoIP Telecom Provider Networks

11. It was further part of the conspiracy that defendant PENA and Moore would use computers to execute a "Brute Force" attack by flooding VoIP Telecom Providers with a multitude of

test calls, each carrying a different Prefix. The "Brute Force" attack would progress by continuously cycling through a volume of possible Prefixes until a proprietary Prefix match would be identified and a test call sent by defendant PENA would succeed in penetrating the corresponding network. Through this Brute Force attack, defendant PENA and Moore would acquire the proprietary Prefixes needed to route calls over the networks of the VoIP Telecom Providers.

12. It was further part of the conspiracy that once the coconspirators penetrated the networks of VoIP Telecom Providers, defendant PENA would program the Unsuspecting Intermediaries' networks, as well as the Decoy Servers, to insert the illegally obtained proprietary Prefix into calls of the Telecom Customers for routing.

13. It was further part of the conspiracy that because defendant PENA sent calls to the VoIP Telecom Providers through the Unsuspecting Intermediaries' networks and the Decoy Servers, the VoIP Telecom Providers would be unable to identify the true sender of the calls for billing purposes. Consequently, the VoIP Telecom Providers incurred an aggregate loss of more than $1.4 million in a span of under one year without being able to identify and bill defendant PENA, Fortes Telecom and Miami Tech.

OVERT ACTS

14. In furtherance of the conspiracy and to effect its unlawful object, defendant PENA and his coconspirators committed and caused to be committed the following overt acts in the District of New Jersey and elsewhere:

a. On or about July 5, 2005, using the alias "Jake Hamilton," Moore sent an e-mail to FDCServers, a computer server provider located in or around Chicago, Illinois, for the purpose of establishing a computer server to disguise the origin of unauthorized telephone call traffic routed over the networks of the VoIP Telecom Providers.

b. On or about July 25, 2005, defendant PENA caused a VoIP telephone call to be transmitted via the internet through routers operated by O.H., located in or around Ryebrook, New York, to N.P., located in or around Newark, New Jersey.

c. On or about October 6, 2005, Moore registered with a computer server provider located in or around Los Angeles, California, to host the server of the Miami Tech & Consulting, Inc. website, http://www.miamitac.com.

d. In or about May 2005, defendant PENA hacked into the external router of O.H. and reprogrammed O.H.'s router to accept VoIP telephone calls and to direct them to the VoIP Telecom Providers that he had previously infiltrated, including N.P., a Newark, New Jersey company.

In violation of Title 18, United States Code, Section 371.

COUNT 2
WIRE FRAUD RELATED TO ROUTING CALLS VIA O.H.
(18 U.S.C. § 1343)

1. The allegations set forth in paragraphs 1 and 2, and 4 through 14 of Count One of this Indictment are realleged and incorporated herein.

2. Between on or about July 10, 2005 and on or about July 25, 2005, defendant PENA caused his Telecom Customers' VoIP telephone calls to be transmitted via the internet through routers operated by O.H., located in or around Ryebrook, New York, to N.P., located in or around Newark, New Jersey. To do so, defendant PENA obtained, without authorization, the valid proprietary Prefix that N.P. used to identify authorized calls from legitimate customers of N.P. With an identified N.P. proprietary Prefix and the hacked O.H. router, in an approximately three-week period, defendant PENA was able to send approximately 500,000 calls through N.P.'s VoIP telephone network and make it appear as if O.H. was sending the calls.

3. On or about July 25, 2005, in Essex County, in the District of New Jersey and elsewhere, defendant

EDWIN ANDRES PENA
a/k/a "Javier Alejandro Sanchez Rinco,"
a/k/a "David Hauster,"
a/k/a "Renato Moreno"

for the purpose of executing and attempting to execute a scheme and artifice to defraud and to obtain money and property by means

of materially false and fraudulent pretenses, representations, and promises, did knowingly and with intent to defraud transmit and cause the transmission of, by means of wire communications, writings, signs, signals, and sounds in interstate and foreign commerce, namely, electronic transfer of a customer's VoIP telephone calls over the internet from a computer network router of O.H., located in or around Ryebrook, New York, to a computer network of N.P., located in or around Newark, New Jersey, without authorization.

In violation of Title 18, United States Code, Sections 1343 and 2.

COUNTS 3 THROUGH 11
WIRE FRAUD RELATED TO ROUTING CALLS
ON THE VoIP TELECOM PROVIDERS
(18 U.S.C. § 1343)

1. The allegations set forth in paragraphs 1 and 2, and 4 through 14 of Count One, and paragraph 2 of Count Two of this Indictment are realleged and incorporated herein.

2. On or about the dates listed below, in Essex County, in the District of New Jersey and elsewhere, defendant

EDWIN ANDRES PENA
a/k/a "Javier Alejandro Sanchez Rinco,"
a/k/a "David Hauster,"
a/k/a "Renato Moreno"

for the purpose of executing and attempting to execute a scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, did knowingly and with intent to defraud transmit and cause the transmission of, by means of wire communications, writings, signs, signals, and sounds in interstate and foreign commerce, namely, on or about the dates listed below, electronic transfer of a customer's VoIP telephone calls over the internet to the provider's computer systems to process and transmit the telephone calls.

COUNT	DATES	Provider
3	July 25, 2005	N.P.
4	July 25, 2005	L.N.
5	July 25, 2005	N.T.
6	August 24, 2005	R.S.
7	January 20, 2006	R.S.
8	January 17, 2006	N.C.
9	August 5, 2006	G.T.
10	April 28, 2006	G.T.T.
11	May 3, 2006	V.E.

In violation of Title 18, United States Code, Sections 1343 and 2.

COUNTS 12 THROUGH 20
COMPUTER FRAUD AND ABUSE
(18 U.S.C. § 1030)

1. The allegations set forth in paragraphs 1 and 2, and 4 through 14 of Count One, and paragraph 2 of Count Two of this Indictment are realleged and incorporated herein.

2. On or about the dates listed below, in Essex County, in the District of New Jersey and elsewhere, defendant

EDWIN ANDRES PENA
a/k/a "Javier Alejandro Sanchez Rinco,"
a/k/a "David Hauster,"
a/k/a "Renato Moreno"

did knowingly and with intent to defraud access protected computers of the entities listed below, without authorization, and exceed authorized access, namely by obtaining and using proprietary Prefixes of VoIP Telecom Providers, and by means of such conduct furthered the intended fraud and obtained things of value:

COUNT	DATES	Entity
12	July 25, 2005	N.P.
13	July 25, 2005	L.N.
14	July 25, 2005	N.T.
15	August 24, 2005	R.S.
16	January 20, 2006	R.S.
17	January 17, 2006	N.C.
18	August 5, 2006	G.T.
19	April 28, 2006	G.T.T.
20	May 3, 2006	V.E.

In violation of Title 18, United States Code, Sections 1030(a)(4) and 2.

A TRUE BILL

Ralph J. Marra, Jr.

RALPH J. MARRA, JR.
ACTING UNITED STATES ATTORNEY

CASE NUMBER: 09-103 (SDW)

United States District Court
District of New Jersey

UNITED STATES OF AMERICA

v.

EDWIN ANDRES PENA
a/k/a "Javier Alejandro Sanchez Rinco,"
a/k/a "David Hauster,"
a/k/a "Renato Moreno"

INDICTMENT FOR

18 U.S.C. §§ 371, 1030, 1343, and 2

RALPH J. MARRA, JR.
ACTING U.S. ATTORNEY NEWARK, NEW JERSEY

EREZ LIEBERMANN
ASSISTANT U.S. ATTORNEY
(973) 645-2874

USAO#2005R00946